UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/887,599	06/22/2001	Peter Yianilos	500578.2001	7240

7590 03/16/2005

STEPHEN M. CHINN
REED SNITH LLP
599 LEXINGTON AVENUE
29TH FLOOR
NEW YORK, NY 10022

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/887,599	YIANILOS ET AL.	
	Examiner	Art Unit	
	Benjamin E Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 22 June 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claim 1 recites the limitation "said firewalls" in line 15. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by England, U.S. Patent No. 6,775,779. Referring to claims 1, 8, 17, 19, 20, England discloses a computer system for content protection wherein the operating system is authenticated during the boot process before it is loaded (Col. 2, lines 16-40), which meets the limitations of a computer platform having hardware capable of authenticating an operating system to be loaded on said hardware

and preventing said operating system from being loaded onto said hardware when said operating system is not authenticated. The system uses a "secure pages" architecture that is capable of running designated processes, libraries, or other software components (Col. 2, lines 65-67), which meets the limitation of said hardware having memory in which application programs and object files can be stored. This "secure pages" architecture runs the programs at a higher level of protection. For example, rights management operating system modules, communications drivers, and video decoding applications programs can run in protected memory that is not accessible by other OS modules and device drivers and by other applications outside the OS (Col. 3, lines 1-9), which meets the limitations of said operating system capable of creating a firewall around data in memory pertaining to application programs and object files to control access to said application programs and object files, and said firewall around said data in memory being capable of allowing said application programs to access said data in memory when approval of access is obtained from said application program and from said data in memory because Applicant defines the "firewall" as an arrangement in the computer platform that performs memory management in the form of access control. The system can decrypt and authentication encrypted content that is provided to the system (Col. 8, line 64 – Col. 9, line 29), which meets the limitation of an input interface connected to said platform to allow input data to be received by said platform and said operating system capable of decrypting said input data and of authenticating said input data. The system further provides for secure encrypted sessions wherein encrypted content is transmitted (Col. 11, line 55 – Col. 12, line 5), which meets the limitation of an output interface connected to said platform to allow said platform to transmit output data out of said platform, and said output data being encrypted when transmitted.

Referring to claims 2, 18, England discloses that the operating system authentication uses digital signatures for verification (Col. 2, lines 16-40).

Referring to claims 3, 9, England discloses that the content is decrypted using secret keys (Col. 11, lines 6-30), which meets the limitation of operating system decrypts said input data with a private decryption key unique to said platform and output data is decrypted with an decryption key associated with said public encryption key.

Referring to claim 4, England discloses that the digital signature is created with a public key (Col. 9, lines 18-20), which meets the limitation of operating system authenticates said input data by verifying a digital signature associated with said input data with a public signature key and input data that is not authenticated by said operating system is classified as insecure data.

Referring to claims 5, 10, England discloses that public keys are used for data encryption (Col. 9, lines 43-55).

Referring to claim 6, England discloses that the digital signature is created with a secret key (Col. 11, lines 6-17).

Referring to claim 7, England discloses a secure handler located in secure memory that controls access to the secure memory (Col. 7, lines 37-49), which meets the limitation of data in memory gives approval for access through an object handler associated with each of said object files when said data in memory pertains to said object files.

Referring to claim 11, England discloses that the authentication procedure can be performed by a hash digest (Col. 9, lines 43-45).

Referring to claim 12, England discloses a computer system for content protection wherein the operating system is authenticated during the boot process before it is loaded (Col. 2,

lines 16-40), which meets the limitations of a receiving platforms, each of said receiving platforms having firmware and an operating system, said firmware authenticating said operating system. The system uses a "secure pages" architecture that is capable of running designated processes, libraries, or other software components (Col. 2, lines 65-67), which meets the limitation of said hardware having memory in which application programs and object files can be stored. This "secure pages" architecture runs the programs at a higher level of protection. For example, rights management operating system modules, communications drivers, and video decoding applications programs can run in protected memory that is not accessible by other OS modules and device drivers and by other applications outside the OS (Col. 3, lines 1-9), which meets the limitations of said operating system capable of creating a firewall around data in memory pertaining to application programs and object files to control access to said application programs and object files, and said firewall around said data in memory being capable of allowing said application programs to access said data in memory when approval of access is obtained from said application program and from said data in memory because Applicant defines the "firewall" as an arrangement in the computer platform that performs memory management in the form of access control. The system can decrypt and authentication encrypted content that is provided to the system (Col. 8, line 64 – Col. 9, line 29), which meets the limitation of a plurality of a sending station, each of said receiving platforms being adapted to receive said application programs, object files, handlers and signatures, an input interface connected to said platform to allow input data to be received by said platform and said operating system capable of decrypting said input data and of authenticating said input data. The system further provides for secure encrypted sessions wherein encrypted content is transmitted (Col. 11, line 55 – Col. 12, line 5),

which meets the limitation of an output interface connected to said platform to allow said platform to transmit output data out of said platform, and said output data being encrypted when transmitted. England discloses that the digital signature is created with a public key (Col. 9, lines 18-20), which meets the limitation of operating system authenticates said input data by verifying a digital signature associated with said input data with a public signature key and input data that is not authenticated by said operating system is classified as insecure data.

Referring to claim 13, England discloses that public keys are used for data encryption (Col. 9, lines 43-55).

Referring to claims 14, 15, England discloses that the digital signature is created with a secret key (Col. 11, lines 6-17).

Referring to claim 16, England discloses that the digital signature is created with a public key (Col. 9, lines 18-20), which meets the limitation of each receiving platform having a plurality of public signature identification keys to correspond to the plurality of secret keys at said sending station.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100